UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,834	03/12/2002	Thomas Breitbach	RIEB.P-44	1508

28752 7590 09/02/2008

LACKENBACH SIEGEL, LLP
LACKENBACH SIEGEL BUILDING
1 CHASE ROAD
SCARSDALE, NY 10583

EXAMINER	
LU, ZHIYU	
ART UNIT	**PAPER NUMBER**
2618	

MAIL DATE	DELIVERY MODE
09/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/936,834	BREITBACH ET AL.	
	Examiner	Art Unit	
	ZHIYU LU	2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 20-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 20-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Affidavits filed on 05/30/2008 under 37 CFR 1.131 is sufficient to overcome HBCI Interface Specification Version 2.1.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 20-38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claims 1 and 37 are objected to because of the following informalities:

In claim 1, insert colon after "the steps of" in line 2.

In claim 37, insert colon after "the steps of" in line 2; insert semicolon after "a mobile station" in line 3.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1, 27, 29 and 37-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 37-38 recite the limitation "the radiotelephone end". There is insufficient antecedent basis for this limitation in the claim. It is confusing to put both “mobile radiotelephone” and “mobile station” in the same claim while they both direct to the same device.

Claim 27 recites the limitation "the generation of a key" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim 29 recites the limitation "the mobile radiotelephone network operator" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 37 recites the limitation "the HBCI gateway" in lines 10-11. There is insufficient antecedent basis for this limitation in the claim. For examination, the Examiner interprets as the communications gateway mentioned in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 20-21, 24-25 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890).

Regarding claim 1, Dahm et al. teach a method for using standardized bank services via mobile radiotelephone, comprising the steps of

transmitting data between a bank server and a mobile station (paragraphs 0020, 0052);

inserting a communications gateway (114 of Fig. 1) into the transmission path between the bank server (104 of Fig. 1, or obviously the other end of 104 of Fig. 2A) and the mobile station (106 of Fig. 1), which carries out a transformation between the transmission method used at the bank end and a transmission method used at the radiotelephone end (paragraph 0024); and

spitting of the customer-end system into two components, the mobile station (106 of Fig. 1) and said communications gateway (114 of Fig. 1).

But, Dennis does not expressly disclose a SIM card of the mobile station.

Vatanen teaches using a SIM card equipped mobile station in a GSM network to communicate with a bank server at the end of a wired dedicated network via a communications gateway (Figs. 2-3, column 2 line 21 to column 3 line 24, column 4 lines 8-38).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate using a SIM card in a GSM network taught by Vatanen into the method of Dahm et al., in order to identify user and verify account.

Regarding claim 37, Dahm et al. teach a method for using standardized bank services via mobile radiotelephone, comprising the steps of

transmitting data between a bank server and a mobile station (paragraphs 0020, 0052);

inserting a communications gateway (114 of Fig. 1) into the transmission path between the bank server (104 of Fig. 1, or obviously the other end of 104 of Fig. 2A) and the mobile station (106 of Fig. 1), which carries out a transformation between the transmission method used at the bank end and a transmission method used at the radiotelephone end (paragraph 0024);

splitting the customer-end system into two component, the mobile station (106 of Fig. 1) and the communications gateway (114 of Fig. 1);

forming two transmission routes, the first between the mobile station and the communications gateway (102 of Fig. 1, wireless) and the second between the communications gateway and a bank server (100 of Fig. 1, landline); and

unpacking a communication protocol by the communications gateway and converting its protocol sequence such that compatibility with a GSM mobile station and a GSM network is obtained so that an exchange of the converted protocol with the GSM mobile station is possible (Figs. 3-4, paragraphs 0024-0026).

But, Dahm et al. do not expressly disclose a SIM card of the mobile station.

Vatanen teaches using a SIM card equipped mobile station in a GSM network to communicate with a bank server at the end of a wired dedicated network via a communications gateway (Figs. 2-3, column 2 line 21 to column 3 line 24, column 4 lines 8-38).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate using a SIM card in a GSM network taught by Vatanen into the method of Dahm et al., in order to identify user and verify account.

Regarding claim 38, Dahm et al. teach a method for using bank services via mobile radiotelephone in which data is transmitted between a bank server and a mobile station (paragraphs 0020, 0052), comprising the steps of:

inserting a communications gateway (114 of Fig. 1) into the transmission path between the bank server (obviously the other end of 104 of Fig. 2A, paragraph 0052) and the mobile station (106 of Fig. 1), which carries out a transformation between the transmission method used at the bank end and a wireless transmission method used at the radiotelephone end (paragraphs 0024, 0052) including a reduction of data transmitted to the mobile station (paragraph 0026, where HDTP uses less data in transmission than HTTP does);

transmitting data between the communications gateway and the mobile station according to the wireless transmission method used at the radio telephone end (102 of Fig. 1); and

transmitting data between the communications gateway and the bank server using the transmission method used at the bank end (100 of Fig. 1, or 104 of Fig. 2A).

For further clarifying, Vatanen teaches using bank services via mobile radiotelephone in which data is transmitted between a bank server (13 of Figs 2-3) and a mobile station (1 of Figs. 2-3), where a communications gateway (4 of Fig. 2, or 7 of Fig. 3) is in between (column 2 line 21 to column 3 line 24).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to recognize and incorporate bank server end of Vatanen into the method of Dahm et al., in order to provide bank service.

Regarding claim 20, Dahm et al. and Vatanen teach the limitation of claim 1.
Dahm et al. and Vatanen teach wherein two transmission routes are formed, first between a SIM card and the communications gateway and second between the communications gateway and a bank server (Airnet & Landnet of Fig. 1 of Dahm et al.).

Regarding claim 21, Dahm et al. and Vatanen teach the limitation of claim 1.
Dahm et al. and Vatanen teach wherein a banking protocol is unpacked by the communications gateway and its protocol sequence is converted such that compatibility with a GSM SIM card and a GSM network is obtained in order for an exchange of the converted protocol with the GSM SIM card is to be possible (paragraph 0024 of Dahm et al., column 2 line 21 to column 3 line 24, column 4 lines 8-38 of Vatanen).

Regarding claim 24, Dahm et al. and Vatanen teach the limitation of claim 1.
Dahm et al. teach wherein between the bank server and the communications gateway a security protocol defined by the communications is applied (HTTPS, paragraph 0025) and between the communications gateway and a SIM card a second security protocol is employed (SUGP, paragraph 0025).

Regarding claim 25, Dahm et al. and Vatanen teach the limitation of claim 24.
Dahm et al. and Vatanen teach wherein the second security protocol corresponds to a protocol reduced in terms of data quantity (paragraph 0026) but equivalent to the communications gateway in terms of security technology (paragraph 0025).

6. Claims 22-23 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890) and Hultgren (US Patent#6868391).

Regarding claim 22, Dahm et al. and Vatanen teach the limitation of claim 1.

Dahm et al. and Vatanen teach wherein a carrier service for the information exchange between said communications gateway and mobile station serves a GSM data transmission service (410 of Fig. 4).

But, Dahm et al. and Vatanen do not expressly disclose Short Message Service, GPRS or USSD in GSM data transmission service.

Hultgren teaches exchanging information with short message service in GSM network (column 13 lines 22-32).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate using short message service to exchange information taught by Hultgren into the method of Dahm et al. and Vatanen, in order to utilize simple GSM data transmission service to exchange information.

Regarding claim 23, Dahm et al. and Vatanen teach the limitation of claim 20.

But, Dahm et al. and Vatanen do not expressly disclose wherein on both routes a cryptographic security is realized.

However, Dahm et al. teach one route uses secure HTTP and the other route use secure UGP (paragraph 0025), wherein secure session may be established by exchanging encryption keys from both sides (paragraph 0054).

Hultgren teaches on both routes a cryptographic security is realized (column 6 lines 38-43, column 12 lines 59-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate having cryptographic security on both routes taught by Hultgren into the method of Dahm et al. and Vatanen, in order to ensure secure transaction.

Regarding claim 36, Dahm et al. and Vatent teach the limitation of claim 1.

But, Dahm et al. and Vatent do not expressly disclose wherein an additional authentication of a subscriber takes place via an identification of his/her mobile connection to carry out an evaluation of a calling line identification.

Hultgren teaches wherein an additional authentication of a subscriber takes place via an identification of his/her mobile connection to carry out an evaluation of a calling line identification (CLI) (column 13 lines 33-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate using CLI for authentication taught by Hultgren into the method of Dahm et al. and Vatent, in order provide authentication.

7. Claims 26-28, 30-31, 34 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890), "HBCI HOMEBANKING COMPUTER INTERFACE – Interface Specification – Version 2.0.1" (hereafter, HBCI), and "At the Coal-face Between Financial Industries and Politics" (hereafter, Interview w/ CG).

For the sake of argument, the following rejection on claim 37 is based on taking HBCI gateway in the interpretation of the claim.

Regarding claim 37, Dahm et al. and Vatanen teach a method for using standardized bank services via mobile telephone as explained in response to claim 37 above.

But, Dahm et al. and Vatanen do not expressly disclose the communications gateway being a HBCI gateway.

HBCI is a well known standardized bank-independent protocol for online banking, developed and in use by German banks, which provides support for multibanking, platform-independent, and DES- and RSA-encryption and -signatures with chip card (HBCI, Chapters I.1, VIII.8.4).

Further, Interview w/ CG teaches that with GSM network anyone could design using one of OFX, Integrion Gold, and HBCI as design preference for adapting European Internet banking standard in the international network banking implementation (pages 1-11, especially 21st-22nd Q&G).

Thus, one of ordinary skill in the art can implement HBCI gateway between the GSM network and the banks (as shown in Interview w/ CG). The implemented network can be used in GSM

mobile network with the European banks. The implemented network will also function necessary step such as splitting the customer-end system into GSM and HBCI. In Dahm et al., the landnet (100 of Fig. 1) would obviously be the HBCI network, and the communications gateway (114 of Fig. 1) would obviously be the HBCI gateway that transforms information between the landnet and the airnet (Fig. 1).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate HBCI gateway into the communications gateway of Dahm et al. and Vatanen as design preference as evidenced by Interview w/ CG, in order to perform online banking with European banks over GSM network.

Regarding claim 26, Dahm et al. and Vatanen teach the limitation of claim 25.

Dahm et al. teach exchanging encryption keys from both sides (paragraph 0054), but Dahm et al. and Vatanen do not expressly disclose wherein a cryptographic keys (Ksms) specific to each subscriber is securely generated and stored in a SIM card for use in the second security protocol after regular SIM card personalization.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach incorporating HBCI gateway into the communication gateway between the bank end and the radiotelephone end as explained in response to claim 37 above.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach a cryptographic key (Ksms) (signature key of HBCI) specific to each subscriber is securely generated and stored in a SIM card (Chip card of Fig. 1 of HBCI; SIM card of Vatanen) for use in the second security protocol after

regular SIM card personalization (HBCI chapters I, VI.3.1.1 Key types), in order to provide security.

Regarding claim 27, Dahm et al. and Vatanen teach the limitation of claim 1.
Dahm et al. teach exchanging encryption keys from both sides (paragraph 0054), but Dahm et al. and Vatanen do not expressly disclose wherein the generation of a key (Ksms) specific to a subscriber is generated in a SIM card by entering an initialization PIN on a mobile telephone.
Dahm et al., Vatanen, HBCI, and Interview w/ CG teach the generation of a key (Ksms) specific to a subscriber is generated in a SIM card (apply explanation in response to claim 26 above) by entering an initialization PIN on a mobile telephone (HBCI chapter VI.3; column 2 lines 24-26, column 3 lines 42-55 of Vatanen), in order to provide security.

Regarding claim 28, Dahm et al., Vatanen, HBCI, and Interview w/ CG teach the limitation of claim 27.
HBCI teaches wherein a subscriber is informed per PIN letter by the bank of a PIN for generating the key (Ksms) (chapter VI.3.1.3.2 Initial key distribution, in writing from the bank).

Regarding claim 30, Dahm et al. and Vatanen teach the limitation of claim 1.
But, Dahm et al. and Vatanen do not expressly disclose wherein before subscription to a service a subscriber receives the data of his bank including an initialization PIN.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach incorporating HBCI gateway into the communication gateway between the bank end and the radiotelephone end as explained in response to claim 37 above.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach wherein before subscription to a service a subscriber receives the data of his bank including an initialization PIN (HBCI, User ID of III.1.1, VI.3.1.3.2 Initial key distribution), in order to obtain initialization PIN.

Regarding claim 31, Dahm et al., Vatanen, HBCI, and Interview w/ CG teach the limitation of claim 30.

HBCI teaches a cryptographic method of generating the key through triple DES using country code (local PIN), bank code (routing number), user ID (account number), key type, key number, and version number (VI.3.1.1, II.5.3.2), which means during the initialization of an application, i.e. during subscription, with the aid of the KIV from initialization PIN, the key Ksms is generated through triple DES using the local PIN, the bank routing number and an account number.

Regarding claim 34, Dahm et al. and Vatanen teach the limitation of claim 1.

But, Dahm et al. and Vatanen do not expressly disclose wherein the authentication of the two involved sites, mobile radiotelephone subscriber and said communications gateway, takes place by knowledge of the initialization PIN exchanged in writing.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach incorporating HBCI gateway into the communication gateway between the bank end and the radiotelephone end as explained in response to claim 37 above.

Dahm et al., Vatanen, HBCI, and Interview w/ CG teach wherein the authentication of the two involved sites, mobile radiotelephone subscriber and said communications gateway, takes place by knowledge of the initialization PIN exchanged in writing (VI.3.1.3.2 of HBCI), in order to proceed authentication of each other.

8. Claims 29 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890) and Atalla (US Patent#4288659).

Regarding claim 29, Dahm et al. and Vatanen teach the limitation of claim 1.

Dahm et al. teach exchanging encryption keys from both sides (paragraph 0054), but Dahm et al. and Vatanen do not expressly disclose wherein during a card personalization by the mobile radiotelephone network operator together with a bank application, an initialization key KIV, derived from a master key and a SIM card-individual number, for generating a Ksms specific to the subscriber is applied onto a plurality of SIM cards.

Atalla teaches generating an initialization key based on a secret code (master key) known by both authorized individual and the bank and an identification of the terminal for generating the session key specific to the terminal user (column 1 line 45 to column 2 line 27), where applying

the key generating method would have been obvious to one of ordinary skill in the art to apply on other cards as well.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key from a master key and a hardware individual number taught by Atalla into the method of Dahm et al. and Vatanen, in order to provide both user and hardware authentication in initialization.

Regarding claim 33, Dahm et al. and Vatanen teach the limitation of claim 1.

But, Dahm et al. and Vatanen do not expressly disclose the generation of an initialization PIN takes place at the communications gateway and this is transferred to the bank server.

However, it is known that the gateway is a mid-node for authentication and conversion for user data before communicating with the bank. So, the gateway would be the one who masters security with the user and the bank, which would have been obvious to one of ordinary skill in the art to recognize that having the gateway to generate initialization PIN is secure and convenient. Then initialized PIN can be transferred to the bank so that the bank can inform user the initialization key since the bank is the one who authorize the service.

Atalla teaches the generation of the initialization PIN takes place at a mid-node gateway terminal between user and central server, wherein the mid-node gateway terminal must be initialized in the first operating cycle (column 1 line 45 to column 2 line 27, column 2 lines 64-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key in mid-node taught by Atalla into the

method of Dahm et al. and Vatanen, in order to provide secured user initialization and authentication in the communications gateway.

9. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890), "HBCI HOMEBANKING COMPUTER INTERFACE – Interface Specification – Version 2.0.1" (hereafter, HBCI), "At the Coal-face Between Financial Industries and Politics" (hereafter, Interview w/ CG), and Fujioka (JP10-242957).

Regarding claim 32, Dahm et al., Vatanen, HBCI, and Interview w/ CG teach the limitation of claim 27.

But, Dahm et al., Vatanen, HBCI, and Interview w/ CG do not expressly disclose wherein in the generation of the Ksms in the communications gateway an initialization PIN is transferred to a gateway operator.

Fujioka teaches transferring an initial key to server for generating another key (abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate transferring initialization PIN to server for generating a key taught by Fujioka into the modified method of Dahm et al., Vatanen, HBCI, and Interview w/ CG, in order to authenticate key generation for corresponding client.

10. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dahm et al. (US2001/0014615) in view of Vatanen (US Patent#6169890) and Elgamal et al. (US Patent#5657390).

Regarding claim 35, Dahm et al. and Vatanen teach the limitation of claim 1.

But, Dahm et al. and Vatanen do not expressly disclose between mobile radiotelephone network operator and communications gateway operator a master key is exchanged.

Elgamal et al. teach between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged (column 7 lines 41-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate exchanging master key taught by Elgamal et al. into the method of Dahm et al. and Vatanen, in order for both client and server to produce session keys for encrypt/decrypt data during communication.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ZHIYU LU whose telephone number is (571)272-2837. The examiner can normally be reached on Weekdays: 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on (571) 272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Z. L./
Examiner, Art Unit 2618

/Nay A. Maung/
Supervisory Patent Examiner, Art Unit 2618

Zhiyu Lu
August 28, 2008